Arab Republic of Egypt

Ministry of Communications and Information Technology

E-Government

Code of Practice for Information Security Management



Preface

The information in this document is **E-Government confidential**, and cannot be reproduced or redistributed in any way, shape, or form without prior written consent from E-Government Workgroup Head.

Document Control

Distribution

Document Name:	E-Government Code of practice for information security management
Document Scope:	This standard gives guidelines for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization.
Issue Code:	
Issue Date:	
Status:	Draft

Version Control

Version	Date	Comments
1.0	23.04.2002	
1.3	01.09.2002	

Control Statement

This document will be valid until a further issue is released, the recent issue shall supersede the older one.

Approvals

Level	Title	Signature	Date
Author:			
Verified By:			
Authorized By:			
Issue Date:			

Confidentiality Level

High [X] **Medium** [ ] **Low** [ ] **Public** [ ]

Distribution List

E-Government Workgroup

Table of Contents

INTRODUCTION

What is information security?

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is characterized here as the preservation of:

a) ***Confidentiality***: ensuring that information is accessible only to those authorized to have access;
b) ***Integrity:*** safeguarding the accuracy and completeness of information and processing methods;
c) ***Availability:*** ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

Why information security is needed

Information and the supporting processes, systems and networks are important business assets. Confidentiality, integrity and availability of information may be essential to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image. Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Dependence on information systems and services means organizations are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increases the difficulty of achieving access control. The trend to distributed computing has weakened the effectiveness of central, specialist control. Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the organization. It may also require participation from suppliers, customers or shareholders. Specialist advice from outside organizations may also be needed.

Information security controls are considerably cheaper and more effective if incorporated at the requirements specification and design stage.

How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources.

The first source is derived from assessing risks to the organization. Through risk assessment threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

The second source is the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy.

The third source is the particular set of principles, objectives and requirements for information processing that an organization has developed to support its operations.

Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. Risk assessment techniques can be applied to the whole organization, or only parts of it, as well as to individual information systems, specific system components or services where this is practicable, realistic and helpful.

Risk assessment is systematic consideration of:

a) The business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;
b) The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

The results of this assessment will help guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

It is important to carry out periodic reviews of security risks and implemented controls to:

a) Take account of changes to business requirements and priorities;
b) Consider new threats and vulnerabilities;
c) Confirm that controls remain effective and appropriate.

Reviews should be performed at different levels of depth depending on the results of previous assessments and the changing levels of risk that management is prepared to accept. Risk assessments are often carried out first at a high level, as a means of prioritizing resources in areas of high risk, and then at a more detailed level, to address specific risks.

Selecting controls

Once security requirements have been identified, controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this document or from other control sets, or new controls can be designed to meet specific needs as appropriate. There are many different ways of managing risks and this document provides examples of common approaches. However, it is necessary to recognize that some of the controls are not applicable to every information system or environment, and might not be practicable for all

organizations. As an example, 9.7 and 12.1 describe how system use can be monitored and evidence collected. The described controls e.g. event logging might conflict with applicable legislation, such as privacy protection for customers or in the workplace.
Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Non-monetary factors such as loss of reputation should also be taken into account.
Some of the controls in this document can be considered as guiding principles for information security management and applicable for most organizations. They are explained in more detail below under the heading "Information security starting point".

Information security starting point

A number of controls can be considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security.
Controls considered to be essential to an organization from a legislative point of view include:

a) Data protection and privacy of personal information;
b) Safeguarding of organizational records;
c) Intellectual property rights;

Controls considered to be common best practice for information security include:

a) Information security policy document;
b) Allocation of information security responsibilities;
c) Information security education and training;
d) Reporting security incidents;
e) Business continuity management.

These controls apply to most organizations and in most environments. It should be noted that although all controls in this document are important, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk assessment.

Critical success factors

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

a) Security policy, objectives and activities that reflect business objectives;
b) An approach to implementing security that is consistent with the organizational culture;
c) Visible support and commitment from management;
d) A good understanding of the security requirements, risk assessment and risk management;
e) Effective marketing of security to all managers and employees;
f) Distribution of guidance on information security policy and standards to all employees and contractors;
g) Providing appropriate training and education;
h) A comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidance. Not all of the guidance and controls in this code of practice may be applicable.

Furthermore, additional controls not included in this document may be required. When this happens it may be useful to retain cross-references which will facilitate compliance checking by auditors and business partners.

1 SCOPE

This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.

Recommendations from this standard should be selected and used in accordance with applicable laws and regulations.

2 TERMS AND DEFINITIONS

For the purposes of this document, the following definitions apply.

Information security

Preservation of confidentiality, integrity and availability of information.

- **Confidentiality**
  - Ensuring that information is accessible only to those authorized to have access.
- **Integrity**
  - Safeguarding the accuracy and completeness of information and processing methods.
- **Availability**
  - Ensuring that authorized users have access to information and associated assets when required.

Risk assessment

Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

Risk management

Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost.

3 SECURITY POLICY

3.1 Information security policy

Objective: To provide management direction and support for information security.

Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

- Information security policy document

  A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security. As a minimum, the following guidance should be included:

  a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);
  b) a statement of management intent, supporting the goals and principles of information security;
  c) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, for example:
     1) compliance with legislative and contractual requirements;
     2) security education requirements;
     3) prevention and detection of viruses and other malicious software;
     4) business continuity management;
     5) consequences of security policy violations;
  d) a definition of general and specific responsibilities for information security management, including reporting security incidents;
  e) References to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

  This policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

- Review and evaluation

  The policy should have an owner who is responsible for its maintenance and review according to a defined review process. That process should ensure that a review takes place in response to any changes affecting the basis of the original risk assessment, e.g. significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure.

  There should also be scheduled, periodic reviews of the following:

  a) the policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents;
  b) cost and impact of controls on business efficiency;
  c) Effects of changes to technology.

4 ORGANIZATIONAL SECURITY

4.1 Information security infrastructure

Objective: To manage information security within the organization.

A management framework should be established to initiate and control the implementation of information security within the organization.

Suitable management fora with management leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security should be encouraged, e.g. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, and specialist skills in areas such as insurance and risk management.

4.2 Security of third party access

Objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties.

Access to the organization's information processing facilities by third parties should be controlled. Where there is a business need for such third party access, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in a contract with the third party.

Third party access may also involve other participants. Contracts conferring third party access should include allowance for designation of other eligible participants and conditions for their access. This standard could be used as a basis for such contracts and when considering the outsourcing of information processing.

All requests for third party connections must be made using the Third Party Connection Request. The resulting case will be assigned to the appropriate network support team. A web-based case generation form will be established to help automate the process and to ensure the all correct information is submitted at the time of the request. The required information is outlined in Third Party Connection Request - Information Requirements Document. All information requested on this form must be completed prior to approval and sign off.

All third-party connection requests must have a VP level signature for approval. In some cases approval may be given at a lower level with pre-authorization from the appropriate VP. Also, all partnering companies must complete at sign any paperwork as required by the Legal Department. As a part of the request and approval process, the technical and administrative contact for the partnering company will be required to read and sign the Third Party Connection Acceptable Use Policy and any additional forms.

4.3 Outsourcing

Objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

Outsourcing arrangements should address the risks, security controls and procedures for information systems, networks and/or desk top environments in the contract between the parties.

4.4 Organizational security checklist

	Yes	No
Is there any management framework for controlling and implementing security?		
Security management forum exist (Steering committee)		
Are responsibilities well assigned to each of the steering committee members?		
Is there a security working team?		
Is there a well-defined responsibility to the security team?		
Is there any management authorization process for new information processing facilities?		
Is there any in-house information security experienced adviser?		
Is there a written policy for organizational security structure?		
Is there any independent revision for security policies?		
Is there any third party access?		
Are the reasons of this access identified and well documented?		
Are the risks of such access has been evaluated and documented?		
Are the proper controls in place?		
Are the security requirements well documented in the entire third party contract?		
Is there any outsourcing activities take place?		
Are the risks of outsourcing identified and well documented?		
Are security requirements well documented in all of the outsourcing contracts?		

5 ASSET CLASSIFICATION AND CONTROL

5.1 Accountability for assets

Objective: To maintain appropriate protection of organizational assets.

All major information assets should be accounted for and have a nominated owner.

Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

5.2 Information classification

Objective: To ensure that information assets receive an appropriate level of protection.

Information should be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification system should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.

5.3 Asset classification and control security checklist

	YES	NO
Is there an accurate inventory of IT assets in place? - Information assets; - Software assets; - Physical assets; - Services.		
Is there a process in place to keep it up to date?		
Is information classified to identify the relative importance to the business?		
Is there a set of procedures for controlling and processing information in accordance with the classification scheme adopted? - Copying; - Storage; - Transmission by post, fax, and electronic mail; - Transmission by spoken word, including mobile phone, voicemail, answering machines; - Destruction.		

6 PERSONNEL SECURITY

6.1 Security in job definition and resourcing

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

Security responsibilities should be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment.

Potential recruits should be adequately screened, especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality (non-disclosure) agreement.

6.2 User training

Objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.

Users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

6.3 Responding to security incidents and malfunctions

Objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

Incidents affecting security should be reported through appropriate management channels as quickly as possible.

All employees and contractors should be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of organizational assets. They should be required to report any observed or suspected incidents as quickly as possible to the designated point of contact. The organization should establish a formal disciplinary process for dealing with employees who commit security breaches. To be able to address incidents properly it might be necessary to collect evidence as soon as possible after the occurrence (see 12.1.7).

6.4 Personnel security checklist

	Yes	No
Do human resources take care of Security responsibilities for staff in their job application?		
Is there are any Confidentiality or non-disclosure agreements used in the organization for the employees to sign as part of their initial terms and conditions of employment?		
Is there is any unique individual identifier for each user?		
Is there are Policies and procedures in place for Authentication? - Change passwords often (enforced by system) - Weak passwords not allowable - System stores password encrypted - Token card plus password or PIN - Biometric (fingerprint, retinal scan, etc.) - Identification systems/I.D. badges - Different security for terminals in different locations - Account canceled when employee leaves - Emergency access procedures for forgotten password		
Are these Policies and procedures strictly enforced (even fines)?		
Are there any Policies and procedures in place for assurance of software discipline? - Virus checking all files - Virus checking electronic mail - Control PC software loading - Network software periodic census - Version control / Change control in use		
Are these Policies and procedures strictly enforced (even fines)?		
Is there is someone assigned to conduct a thorough pre-employment screening for all personnel?		
Screening done on all levels?		
Are all references thoroughly checked?		

Are investigative tools such as a polygraph, special tests, or a combination of devices used in pre-employment screening?		
Do supervisors provide an effective level of supervision at all levels?		
Is there a good level of surveillance and vigilance in critical areas?		
Are personnel effectively evaluated in the handling of sensitive materials?		
Are all rules, policies, and procedures enforced?		
Is there an effective security education program?		
Are there any possible warning signs of potential problems with personnel in critical areas (ex. Personnel making threats)?		
Do they back up that commitment with funding for security training?	`	
Is there a mandatory security-training program for system administrators?		
Does that training program include details on configuring and supporting your security policy?		
Do formal security training policies exist?		
Do the policies address a quick, systematic emergency action plan in the event your system has been compromised?		
Are all employees-including executive managers- trained on their security responsibilities for the company?		
Does a framework exist for developing and continuing security awareness and responsiveness?		
Is there are any policies, and procedures for reporting the different types of incident (security breach, threat, weakness or malfunction)?		
When a security violation occurs, is it documented?		
Is there are any mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored?		
Is there are any type of formal disciplinary process for employees who have violated organizational security policies and procedures?		

7 PHYSICAL AND ENVIRONMENTAL SECURITY

7.1 Secure areas

Objective: To prevent unauthorized access, damage and interference to business premises and information.

Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference.

The protection provided should be commensurate with the identified risks. A clear desk and clear screen policy is recommended to reduce the risk of unauthorized access or damage to papers, media and information processing facilities.

7.2 Equipment security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

Equipment should be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

7.3 General controls

Objective: To prevent compromise or theft of information and information processing facilities.

Information and information processing facilities should be protected from disclosure to, modification of or theft by unauthorized persons, and controls should be in place to minimize loss or damage.

7.4 Physical and environmental security checklist

	Yes	No
Are the reasons of any type of physical access identified and well documented?		
Are the risks of such access has been evaluated and documented? (Risk Assessment)		
Are the proper controls in place to minimize loss or damage? - Theft; - Fire; - Explosives; - Smoke;		

- Water (or supply failure); - Dust; - Vibration; - Chemical effects; - Electrical supply interference; - Electromagnetic radiation.		
Is there is any regular revision and updated for access rights to secure areas?		
What type of security for Support functions and equipment? - Photocopiers; - Fax Machines.		
Is there is any type of intruder detection systems installed, and are there any procedures for testing it regularly?		
What type of policies, procedures for third party support services personnel to access secure areas or sensitive information processing facilities?		
What is the policy, procedure for using photographic, video, audio or other recording equipment in the premises?		
Is there are a special areas for delivery and loading and what type of controls on theses areas?		
What are the policies, procedures for equipment siting and protection?		
Is there is a policy towards eating, drinking and smoking on in proximity to information processing facilities?		
What types of procedures are taken in case of a disaster happening in nearby premises?		
What are the different types of equipment protection against power failures and other electrical anomalies?		
Are the proper controls in place to protect power and telecommunications cabling carrying data or supporting information services?		
Are the proper controls in place for equipment maintenance?		
What are the guidelines for using any equipment outside an organization's premises for information processing? - Personal computers; - Organizers;		

- Mobile phones; - Paper or other form.		
What is the policy for disposal or re-use of equipment?		
Is there is a clear desk policy, clear screen policy, and what is the relation to information security classifications?		
Are the proper controls in place for removal of property? - Equipment; - Information; - Software.		

8 COMMUNICATION AND OPERATIONS MANAGEMENT

8.1 Operational procedure and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.
Responsibilities and procedures of the management and operation of all information processing facilities should be established.

8.2 System planning and acceptance

Objective: To minimize the risk of systems failures.
The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

8.3 Protection against malicious software

Objective: To protect the integrity of software and information. Precautions are required to prevent and detect the introduction of malicious software.
Users should be made aware of the dangers of unauthorized or malicious software,
And managers should, where appropriate, introduce special controls to detect or prevent.

8.4 Housekeeping

Objective: To maintain the integrity and availability of information processing and Communication services.

8.5 Network management

Objective: To ensure the safeguarding of information in networks and the protection of the Supporting infrastructure.
The security management of networks which may span organizational boundaries requires attention. Additional controls may also be required to protect sensitive data passing over public networks.

8.6 Media handling and security

Objective: To prevent damage to assets and interruptions to business activities.
Media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media (such as tapes, disks, cassettes, etc), input/output data and system documentation from damage, theft and unauthorized access.

8.7 Exchanges of information and software

Objective: To prevent loss, modification or misuse of information exchanged between organizations.
Exchanges of information and software between organizations should be controlled, and should be compliant with any relevant legislation. Procedures and standards to protect information and media in transit should be established. The business and security Implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

8.8 Communication and operations management security checklist

	Yes	No
Is there is a formal documents for operating procedures and changes should be authorized by management.		
Are the proper controls in place for updating operating procedures document?		
Are the proper controls in place for changes to information processing facilities and systems?		
Are the proper controls in place for Incident management responsibilities and procedures?		
Are the proper controls in place for segregation of duties?		
Are the proper controls in place for separating development, test and operational facilities?		
Are the proper controls in place for the use of an external contractor to manage information processing facilities?		
Is there is any document for capacity planning?		
What are the criteria for accepting a new information systems, upgrades and new versions and what are the suitable tests of the system carried out prior to acceptance?		
What are the Detection and prevention controls to protect against malicious software and is there is any appropriate user awareness procedures implemented?		
Are the proper controls in place for information Back-up?		
Is there is a log for the activities of the operational staff?		
Is there are any regular, independent checks for Operator logs against operating procedures?		
What are the rules for handling reported fault logging?		
Are the proper controls in place to ensure the security of data in networks, and the protection of connected services from unauthorized access (Internal and External)?		
What are the procedures for the management of removable computer media, such as tapes, disks, cassettes and printed reports?		
What are the procedures for the secure disposal of media?		

What are the procedures for the handling and storage of information?		
Are the proper controls in place to protect system documentation from unauthorized access?		
Does the security content of information and software exchange agreement reflect the sensitivity of the business information involved?		
Are the proper controls in place to safeguard computer media being transported between sites?		
Are the proper controls in place to secure Electronic Commerce?		
Are the proper controls in place to reduce security risks created by electronic mail?		
Is there a clear policy regarding the use of electronic mail?		
Is there a policy for publicly available system?		
Is there a clear policy statement of the procedures staff is expected to follow in using voice, facsimile and video communications?		

9 ACCESS CONTROL

9.1 Business requirement for access control

Objective: To control access to information.

Access to information, and business processes should be controlled on the basis of business and security requirements. This should take account of policies for information dissemination and authorization.

9.2 User access management

Objective: To prevent unauthorized access to information systems.

Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

9.3 User responsibilities

Objective: To prevent unauthorized user access.

The co-operation of authorized users is essential for effective security. Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

9.4 Network access control

Objective: Protection of networked services.

Access to both internal and external networked services should be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring:

a) Appropriate interfaces between the organization's network and networks owned by other organizations, or public networks;
b) Appropriate authentication mechanisms for users and equipment;
c) Control of user access to information services.

9.5 Operating system access control

Objective: To prevent unauthorized computer access.

Security facilities at the operating system level should be used to restrict access to computer resources. These facilities should be capable of the following:

a) Identifying and verifying the identity, and if necessary the terminal or location of each authorized user;
b) Recording successful and failed system accesses;
c) Providing appropriate means for authentication; if a password management system is used, it should ensure quality passwords;
d) Where appropriate, restricting the connection times of users.

Other access control methods, such as challenge-response, are available if these are justified on the basis of business risk.

9.6 Application access control

Objective: To prevent unauthorized access to information held in information systems.

Security facilities should be used to restrict access within application systems. Logical access to software and information should be restricted to authorized users. Application systems should:

a) control user access to information and application system functions, in accordance with a defined business access control policy;
b) provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls;
c) not compromise the security of other systems with which information resources are shared;
d) Be able to provide access to information to the owner only, other nominated authorized individuals, or defined groups of users.

9.7 Monitoring system access and use

Objective: To detect unauthorized activities.

Systems should be monitored to detect deviation from access control policy and record monitorable events to provide evidence in case of security incidents. System monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model (see 9.1) to be verified.

9.8 Mobile computing and Teleworking

Objective: To ensure information security when using mobile computing and Teleworking facilities.

The protection required should be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of Teleworking the organization should apply protection to the Teleworking site and ensure that suitable arrangement are in place for this way of working.

9.9 Access control security checklist

	Yes	**No**
Is there a clear policy statement of the procedures for access control rules and rights for each user or group of users?		
Is there are formal procedures in place to control the allocation of access rights to information systems and services? - User registration - Privilege management - User password management		
Is there a regular process to review users' access rights by		

management?		
Is there a policy document to define user's responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment?		
Is there a security practice for the users to follow in the selection and use of passwords?		
What type of protection that user should ensure for unattended equipment?		
Is there a clear policy concerning the use of networks and network services?		
Are the proper controls in place to enforced path which is based on the business access control policy?		
What are different types of authentication method for external connections?		
What are different types of Node authentication method?		
What is the appropriate security mechanism to protect remote diagnostic ports?		
Are the proper controls in place within the network, to segregate groups of information services, users and information systems?		
Are the proper controls in place requiring the incorporation of controls to restrict the connection capability of the users?		
Are the proper controls in place require the incorporation of routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications?		
Is there a clear description of the security attributes of all services used?		
Are the proper controls in place to use the security facilities at the operating system level which should be used to restrict access to computer resources? - Automatic terminal identification - Terminal log-on procedure - User identification and authentication - Password management system - Use of system utilities - Duress alarm to safeguard users		

- Terminal time-out - Limitation of connection time		
Are the proper controls in place to use the security facilities to restrict access within application systems? - Information access restriction - Sensitive system isolation		
What are the different types of monitoring system access and use? - Event Logging - Monitoring system use - Clock synchronization		
Is there a policy that takes into account the risks of working with mobile computing facilities, in particular in unprotected environments?		
Is there are any needs for any kind of Teleworking activities?		
Is there a policy, procedures and standards to control Teleworking activities?		

10 SYSTEMS DEVELOPMENT AND MAINTENANCE

10.1 Security requirements of systems

Objective: To ensure that security is built into governmental information systems.

This will include infrastructure, business applications and user-developed applications. The design and implementation of the business process supporting the application or service can be crucial for security. The government entity should work closely with the supplying vendor to identify and agree upon security requirements prior to the development of information systems.

The government entity team should make sure that all security requirements, including the need for fallback arrangements, are identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

10.2 Security in application systems

Objective: To prevent loss, modification or misuse of government data in application systems.

Appropriate controls and audit trails or activity logs should be designed into government application systems, including user written applications. These should include the validation of input data, internal processing and output data.

Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical governmental assets or information. Such controls should be determined on the basis of security requirements and risk assessment.

10.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information.

Cryptographic systems and techniques should be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

10.4 Security of system files

Objective: To ensure that IT projects and support activities are conducted in a secure manner.

Access to system files should be controlled. Maintaining system integrity should be the responsibility of the government entity to which the application system or software belongs.

10.5 Security in development and support processes

Objective: To maintain the security of government application system software and information.

Project and support environments should be strictly controlled.

Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

10.6 Systems development and maintenance Security Checklist

	Yes	No
Is there are any detailed security requirements analysis and specification? (risk assessment and risk management)		
Are the proper controls, and audit trails or activity logs in place to secure application systems, including user written applications? - Input data validation; - Control of internal processing; - Message authentication; - Output data validation.		
Is there are any Cryptographic systems and techniques used for the protection of information that is considered at risk and for which other controls do not provide adequate protection? - Policy on the use of cryptographic controls; - Encryption; - Digital signatures; - Non-repudiation services; - Key management.		
Are the proper controls in place to secure access to system files? - Control of operational software; - Protection of system test data; - Access control to program source library.		
Are the proper controls in place to ensure the security in the development and support process? - Change control procedures; - Technical review of operating system changes; - Restrictions on changes to software packages; - Hidden channels and Trojan code; - Outsourced software development.		

11 BUSINESS CONTINUITY MANAGEMENT

11.1 Aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.

The consequences of disasters, security failures and loss of service should be analyzed. Contingency plans should be developed and implemented to ensure that business processes can be restored within the required time-scales. Such plans should be maintained and practiced to become an integral part of all other management processes.

Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

11.2 Business Continuity and Contingency Plan (BCCP) Checklist

	Yes	No
Are mission critical business processes identified?		
Are critical timeframes identified for each mission critical business process?		
Are dependencies identified to support each mission critical business process (such as IT applications, staff, telecommunications, electrical power, etc.)?		
Are assumptions documented?		
Is the impact of external factors determined for each mission critical business process (such as legal or policy issues or dependence on external organizations)?		
Are the identified dependencies, external factors, and inputs evaluated to develop risk scenarios for each mission critical business process?		
Is the probability and impact of each risk condition determined for each critical business process?		
Are alternative strategies developed for each mission critical business process?		
Are the materials (such as check stock, forms, etc.) and necessary equipment (such as generators, cell phones, etc.) identified to implement the contingencies?		
Have Emergency Response Teams (ERTs) been established?		
Have roles and responsibilities been clearly documented?		

Are personnel with the appropriate authority been assigned by name to serve on the teams?		
Has or will the plan be tested?		
Has the agency identified the staff involved in executing the alternate strategy?		
Have or will these staff be trained if necessary?		
Has a strategy been developed and documented to return to normal operations?		
Have pre-event planning activities been documented?		
Has a communication strategy been developed and approved to notify staff, providers, vendors, and clients of potential Year 2000 issues?		
Have BCCP notification procedures been documented?		
Have procedures been documented to produce and disseminate hard-copy lists or reports to local offices?		
Are manual procedures documented and up to date?		
Are procedures documented to ensure staff is familiar with using manual procedures?		

12 COMPLIANCE

12.1 Compliance with legal requirements

Objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and for information created in one country that is transmitted to another country (i.e. trans-border data flow).

12.2 Reviews of security policy and technical compliance

Objective: To ensure compliance of systems with organizational security policies and standards.

The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards.

12.3 System audit considerations

Objective: To maximize the effectiveness of and to minimize interference to/from the system audit process.

There should be controls to safeguard operational systems and audit tools during system audits. Protection is also required to safeguard the integrity and prevent misuse of audit tools.

12.4 Compliance security checklist

	Yes	**No**
Are the design, operation, use and management of information systems compliant with legal requirements? - Identification of applicable legislation - Intellectual property rights - Safeguarding of organizational records - Safeguarding of organizational records - Prevention of misuse of information processing facilities - Regulation of cryptographic controls - Collection of evidence		
Is there are regular review for the security of information systems which should be performed against the appropriate security policies and the technical platforms?		
Is there audit for information systems to be compliant with security implementation standards? - Compliance with security policy Technical compliance checking		

Are the proper controls in place to safeguard operational systems and audit tools during system audits, and also to safeguard the integrity and prevent misuse of audit tools?		

13 RESOURCES FOR INTERNET SECURITY INFORMATION

1.1 Web Sites

Project COAST Homepage & Computer Security Archives
http://www.cs.purdue.edu/coast/coast.html

This is a good all-round site for finding security tools such as COPS, Tripwire, SATAN, etc. You can be fairly sure that the source code has not been tampered with, and the Web interface makes it easy to locate what you want. There are also many excellent papers here worth reading.

Spaf's Hotlist
http://www.cs.purdue.edu/homes/spaf/hotlists/csec.html

Dr. Eugene Spafford's computer security hotlist.

CIAC Security Web Site
http://ciac.llnl.gov/

The Livermore Labs security site for government and military sites. They issue alerts similar to CERT alerts. Many of their tools are available to the public, though some are restricted to DOD users.

AUSCERT Information Pages
http://www.auscert.org.au/

AUSCERT is the Australian Computer Emergency Response Team (CERT) team. They have some tools and papers not found at some of the other, American sites, including a very good paper on developing security policies and a veritable book on security in open systems environments.

8lgm: Security Advisories
http://www.8lgm.org

The "Eight Little Green Men" (or is it "Eight-Legged Groove Machine"?) are a self-appointed group of security vigilantes who publish their own advisory announcements for newly discovered security bugs and problems. In addition to their Web site, they also maintain a mailing list.

Telstra Corporation: Computer and Network Security Reference Index
http://www.telstra.com.au/info/security.html

NIST Computer Security Resource Clearinghouse
http://csrc.nist.gov/

The National Institute of Standards and Technology's computer security web site. This site contains information on DES and the proposed Advanced Encryption standards, the Public Key Infrastructure project, and computer security-related Federal Information Processing Standards and Special Publications.

University of California at Davis Computer Security Research Lab
http://seclab.cs.ucdavis.edu/Security.html

Information from on-going research projects in intrusion detection and auditing.

London School of Economics Computer Security Research Center
http://csrc.lse.ac.uk/csrc/csrchome.htm

Resources for Internet Security Information DRAFT
DRAFT 102

Institute for Computer and Telecommunications Systems Policy
http://www.seas.gwu.edu:80/seas/ictsp/

Information relevant to legal issues in computing and the "information superhighway".

World Wide Web Security Issues

WWW Security FAQ	http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html
Rutgers U.	http://www-ns.rutgers.edu/www-security/index.html
HotJava	http://java.sun.com/1.0alpha3/doc/security/security.html
C2 Challenge	http://www.c2.org/hacknetscape/
CGI Security	http://www.cerf.net/~paulp/cgi-security
General WWW FAQ	http://www.boutell.com/faq
CGI FAQ	http://www.best.com/~hedlund/cgi-faq

Router and Network Vendor Sites
http://www.cisco.com
http://www.livingston.com
http://www.baynetworks.com
http://www.network.com
http://www.racal.com/networking.html

Firewall Vendor Sites, by product name

Gauntlet	http://www.tis.com
NetSP	http://www.ibmlink.ibm.com/oi/ann/alet/294774.html
Sidewinder	http://www.sctc.com
Borderware	http://www.border.com
Firewall-1	http://www.checkpoint.com
DEC SEAL	http://www.digital.com
Centri	http://www.cohesive.com
PORTUS	http://www.sccsi.com/lsli/lsli.homepage.html
Eagle	http://www.raptor.com
Black Hole	http://www.milkyway.com
InterLock	http://www.ans.net/security.html
NET1-AccessPlus	http://www.iu.net/n1/
Ascend	http://www.ascend.com

1.2 Ftp Sites

ftp.cisco.com	Cisco product info, sample screening rules, etc
rtfm.mit.edu	MIT archives for USENET newsgroup FAQs
ftp.greatcircle.com	Firewalls info and archives
net.tamu.edu	Texas A&M University (TAMU tools)
ftp.uu.net	UUNET archives

1.3 Usenet News Groups

Computer Security

alt.security	Security issues on computer systems
alt.security.index	Pointers to good stuff in misc.security (Moderated)
comp.risks	Risks to the public from computers & users
comp.security.announce	Announcements from the CERT about security
comp.security.firewalls	Discussion about Internet firewalls
comp.security.misc	Security issues of computers and networks
comp.security.unix	Discussion of Unix security

TCP/IP networking:

comp.protocols.tcp-ip	TCP and IP network protocols

Telecom:

comp.dcom.cellular	
comp.dcom.telecom	Telecommunications digest (Moderated)
comp.dcom.telecom.tech	

Communications, vendor-specific:

comp.dcom.sys.cisco
comp.dcom.sys.wellfleet

Packet networks:

comp.dcom.frame-relay
comp.dcom.isdn
comp.dcom.cell-relay

1.4 Mailing Lists

Firewalls

Registration Address: Send a message to majordomo@greatcircle.com containing the line "subscribe firewalls user@host". This list is moderated by Brent Chapman, president of Great Circle Associates.

Bugtraq

To join, send e-mail to LISTSERV@NETSPACE.ORG and, in the text of your message (not the subject line), write:" SUBSCRIBE BUGTRAQ". This is a full-disclosure list moderated by Aleph1@underground.org.

CERT Advisories

Registration Address: cert-advisory-request@cert.org

CERT Tools

Reflector Address: cert-tools@cert.org
Registration Address: cert-tools-request@cert.org
Resources for Internet Security Information DRAFT
DRAFT 104

Alert
Reflector Address: alert@iss.net
Registration Address: request-alert@iss.net
This list is moderated by Christopher Klaus, president of Internet Security Systems, Inc.

Best of Security
To join, send e-mail to best-of-security-request@suburbia.net with the following in the body of the message: "subscribe best-of-security". This list is moderated (so to speak) by Julian Assange.

1.5 Books

Practical Unix and Internet Security, 2nd Edition
Author Simson Garfinkel and Gene Spafford
Copyright Date 1996
ISBN 1-56592-148-8
Publisher O'Reilly & Associates, Inc.

Firewalls and Internet Security
Author William Cheswick and Steven Bellovin
Publisher Addison Wesley
Copyright Date 1994
ISBN 0-201-63357-4

Building Internet Firewalls
Author Brent Chapman & Elizabeth Zwicky
Publisher O'Reilly & Associates, Inc.
Copyright Date 1995
ISBN 1-56592-124-0

Actually Useful Internet Security Techniques
Author Larry Hughes
Publisher New Riders Press
Copyright Date Sep-95
ISBN 1-56205-508-9

Computer Crime: A Crimefighter's Handbook
Authors David Icove, Karl Seger and William
V St h Publisher O'Reilly & Associates, Inc.
Copyright Date 1995
ISBN 1-56592-086-4

Computer Security Basics
Authors Deborah Russell & G.T. Gangemi Sr.
Publisher O'Reilly & Associates, Inc.
Resources for Internet Security Information DRAFT
DRAFT 105
Copyright Date 1991
ISBN 0-937175-71-4

Security in Computing

Author Charles P. Pfleeger
Publisher Prentice Hall
Copyright Date 1989
ISBN 0-13-798943-1.

Network Security: Private Communication in a Public World
Authors Charles Kaufman, Radia Perlman, and Michael
Speciner
Publisher Prentice Hall
Copyright 1995
ISBN 0-13-061466-1

Unix System Security
Author Rik Farrow
Publisher Addison Wesley
Copyright Date 1991
ISBN 0-201-57030-0

Unix Security: A Practical Tutorial
Author N. Derek Arnold
Publisher McGraw Hill
Copyright Date 1993

Unix System Security: A Guide for Users and Systems Administrators
Author David A. Curry
Publisher Addison-Wesley
Copyright Date 1992
ISBN 0-201-56327-4

Unix Security for the Organization
Author Richard Bryant
Publisher Sams
Copyright Date 1994
ISBN 0-672-30571-2
This list is compiled and maintained by Jody Patilla (jcp@tis.com), a senior security consultant for Trusted Information Systems, in Glenwood, MD.